

On the solution of trivalent decision problems by quantum state identification

Karl Svozil*

*Institut für Theoretische Physik, University of Technology Vienna,
Wiedner Hauptstraße 8-10/136, A-1040 Vienna, Austria*

Josef Tkadlec†

*Department of Mathematics, Faculty of Electrical Engineering,
Czech Technical University, 166 27 Praha, Czech Republic*

Abstract

The trivalent functions of a trit can be grouped into equipartitions of three elements. We discuss the separation of the corresponding functional classes by quantum state identifications.

PACS numbers: 03.67.Lx, 03.65.Ud

Keywords: Trits, trivalent decision problems, quantum state identification

One of the advantages of quantum computation [1, 2, 3, 4, 5, 6, 7] over classical algorithms [8, 9] is due to the fact that in quantum mechanics information can be coded in or “spread among” coherent states in such a way that certain decision problems can be solved by identifying a quantum state which “globally” contains the solution [10, 11]. Thereby, information about single cases are not useful for (and even makes impossible) a decryption of the quantum computation. This feature is not only present in binary decision problems of the usual type, such as Deutsch’s algorithm, but can be extended to d-ary decision problems on dits.

In what follows we shall consider as the simplest of such problems the trivalent functions of trits. We shall group them in three functional classes corresponding to an equipartition of the set of functions into three elements. We then investigate the possibility to separate each of these classes by quantum state identifications [12, 13].

Formally, we shall consider the functions $f: \{-, 0, +\} \rightarrow \{-, 0, +\}$. There are $3^3 = 27$ such functions. The dits will be coded by elements of some orthogonal base in \mathbb{C}^3 . Without loss of generality we may take $(1, 0, 0) = |-\rangle$, $(0, 1, 0) = |0\rangle$, $(0, 0, 1) = |+\rangle$. We will be searching for a function $g: \{-, 0, +\} \rightarrow \mathbb{C}$ such that the images of the mapping $\{-, 0, +\}^{\{-, 0, +\}} \rightarrow \mathbb{C}^3$ defined by

$$f \mapsto g(-)|-\rangle + g(0)|0\rangle + g(+)|+\rangle$$

form the smallest possible number of orthogonal triples.

First, let us show that we may find a function g such that we obtain 3 orthogonal triples. Let the values of g be the $\sqrt[3]{1}$ (in the set of complex numbers) and put, e.g.,

$$g(x) = e^{2\pi i x/3}$$

Let us, for the sake of simplicity and brief notation, identify ‘-’ with ‘-1’ and ‘+’ with ‘+1,’ and denote $\alpha = e^{2\pi i/3}$ and $\bar{\alpha} = \alpha^2$. Hence, $\alpha^3 = 1$, $\alpha\bar{\alpha} = 1$, $\alpha + \bar{\alpha} = -1$. Then, the “quantum oracle” function g is given by the following table:

x	$-$	0	$+$
$g(x)$	$\bar{\alpha}$	1	α

The following triples of functions can be assigned the same vector (except a nonzero multiple)

by the following scheme:

$(-, -, -)$ $(0, 0, 0) \mapsto (1, 1, 1)$ $(+, +, +)$	$(-, -, 0)$ $(0, 0, +) \mapsto (1, 1, \alpha)$ $(+, +, -)$	$(-, -, +)$ $(0, 0, -) \mapsto (1, 1, \bar{\alpha})$ $(+, +, 0)$
$(-, 0, +)$ $(0, +, -) \mapsto (1, \alpha, \bar{\alpha})$ $(+, -, 0)$	$(-, 0, -)$ $(0, +, 0) \mapsto (1, \alpha, 1)$ $(+, -, +)$	$(-, +, -)$ $(0, -, 0) \mapsto (1, \bar{\alpha}, 1)$ $(+, 0, +)$
$(-, +, 0)$ $(+, 0, -) \mapsto (1, \bar{\alpha}, \alpha)$ $(0, -, +)$	$(0, -, -)$ $(+, 0, 0) \mapsto (\alpha, 1, 1)$ $(-, +, +)$	$(+, -, -)$ $(-, 0, 0) \mapsto (\bar{\alpha}, 1, 1)$ $(0, +, +)$

In every column we obtain an orthogonal triple of vectors. Moreover, vectors from different orthogonal triples are apart by the same angle ϕ , for which $\cos \phi = \sqrt{3}/3$.

Now, let us prove by contradiction that the function g cannot be defined in such a way that we obtain at most two orthogonal triples of subspaces. For the sake of contradiction, let us suppose that this proposition is false.

First, all values $g(-), g(0), g(+)$ should be nonzero (if, e.g., $g(-) = 0$ then the vector $(g(-), g(-), g(-))$ assigned to the function $(-, -, -)$ is a zero vector). Hence, we obtain a linear subspace generated by the vector $(1, 1, 1)$.

Second, $g(-), g(0), g(+)$ cannot have the same value (in this case we obtain only one subspace generated by the vector $(1, 1, 1)$).

Let us show that the vectors assigned to the functions $(-, -, 0)$ and $(-, 0, 0)$ are not orthogonal. Indeed, if they are orthogonal, then $0 = g(-)\overline{g(-)} + g(-)\overline{g(0)} + g(0)\overline{g(0)} = |g(-)|^2 + g(-)\overline{g(0)} + |g(0)|^2$ and therefore $g(-)\overline{g(0)}$ is a negative real number. Hence $0 = |g(-)|^2 - |g(-)| \cdot |g(0)| + |g(0)|^2 = (|g(-)| - \frac{1}{2}|g(0)|)^2 + \frac{3}{4}|g(0)|^2$ and therefore $g(0) = 0$ that is impossible.

Let us show that all values $g(-), g(0), g(+)$ are different. Indeed, let, e.g., $g(-) = g(0)$. Analogously as in the previous paragraph we can show that the vectors $(g(-), g(-), g(+))$ and $(g(-), g(+), g(+))$ are not orthogonal. These vectors do not generate the same subspace (otherwise $g(-) = g(0) = g(+)$) and are not multiples of the vector $(1, 1, 1)$, hence at least one of them should be orthogonal to $(1, 1, 1)$. Let, e.g., $(g(-), g(-), g(+))$ is orthogonal to $(1, 1, 1)$. Then $2g(-) + g(+) = 0$ and therefore this vector is a multiple of $(1, 1, -2)$. The subspace making an orthogonal triple with subspaces generated by vectors $(1, 1, 1)$ and $(1, 1, -2)$ is generated by $(1, -1, 0)$. But this is impossible because no coordinate can be zero.

We have shown that the subspaces assigned to functions $(-, -, 0)$ and $(-, 0, 0)$ are not orthogonal and do not coincide (otherwise $g(-) = g(0)$). Hence they do not belong to one orthogonal triple and at least one of them should belong to an orthogonal triple with the space generated by the vector $(1, 1, 1)$. Let, e.g., $(g(-), g(-), g(0))$ is orthogonal to the vector $(1, 1, 1)$. Then $2g(-) + g(0) = 0$. Analogously to previous paragraphs we can show that one of the vectors $(g(-), g(-), g(+))$ and $(g(-), g(+), g(+))$ ($(g(0), g(0), g(+))$ and $(g(0), g(+), g(+))$, resp.) is orthogonal to the vector $(1, 1, 1)$. Since the values of the function g are different, we obtain $g(-) + 2g(+) = 0$ and $2g(0) + g(+) = 0$. The system of equations has the only solution $g(-) = g(0) = g(+) = 0$, which results in a complete contradiction.

In summary we find that we cannot solve the type of trivalent decision problems as discussed above by a single query. Such a behavior has already been observed for the problem to find the parity of an unknown binary function $f : \{0, 1\}^k \rightarrow \{0, 1\}$ of k bits, which turned out to be quantum computationally hard [5, 14, 15, 16, 17]. We conjecture that this hardness increases with the number d of possible states of a single bit.

Acknowledgements

The work was supported by the research plan of the Ministry of Education of the Czech Republic no. 6840770010 and by the grant of the Grant Agency of the Czech republic no. 201/07/1051 and by a the exchange agreement of both of our universities.

* Electronic address: svozil@tuwien.ac.at; URL: <http://tph.tuwien.ac.at/~svozil>

† Electronic address: tkadlec@fel.cvut.cz; URL: <http://math.feld.cvut.cz/tkadlec/>

- [1] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, 2000).
- [2] J. Gruska, *Quantum Computing* (McGraw-Hill, London, 1999).
- [3] C. H. Bennett, E. Bernstein, G. Brassard, and U. Vazirani, “Strengths and Weaknesses of Quantum Computing,” *SIAM Journal on Computing* **26**, 1510–1523 (1997). quant-ph/9701001, URL <http://dx.doi.org/10.1137/S0097539796300933>.
- [4] Y. Ozhigov, “Quantum Computer Can Not Speed Up Iterated Applications of a Black Box,” (1997).

quant-ph/9712051.

- [5] R. Beals, H. Buhrman, R. Cleve, M. Mosca, and R. de Wolf, “Quantum Lower Bounds by Polynomials,” *Journal of the ACM* **48**, 778–797 (2001). quant-ph/9802049, URL <http://dx.doi.org/10.1145/502090.502097>.
- [6] R. Cleve, “An Introduction to Quantum Complexity Theory,” in *Collected Papers on Quantum Computation and Quantum Information Theory*, C. Macchiavello, G. Palma, and A. Zeilinger, eds., pp. 103–127 (World Scientific, Singapore, 2000). quant-ph/9906111.
- [7] L. Fortnow, “One complexity theorist’s view of quantum computing,” *Theoretical Computer Science* **292**, 597–610 (2003). URL [http://dx.doi.org/10.1016/S0304-3975\(01\)00377-2](http://dx.doi.org/10.1016/S0304-3975(01)00377-2).
- [8] H. Rogers, Jr., *Theory of Recursive Functions and Effective Computability* (MacGraw-Hill, New York, 1967).
- [9] P. Odifreddi, *Classical Recursion Theory, Vol. 1* (North-Holland, Amsterdam, 1989).
- [10] N. D. Mermin, “From Cbits to Qbits: Teaching computer scientists quantum mechanics,” *American Journal of Physics* **71**, 23–30 (2003). URL <http://dx.doi.org/10.1119/1.1522741>.
- [11] K. Svozil, “Characterization of quantum computable decision problems by state discrimination,” in *AIP Conference Proceedings*, A. Khrennikov, ed., p. in print (American Institute of Physics, Melville, NY, 2005). quant-ph/0505129, URL inprint.
- [12] N. Donath and K. Svozil, “Finding a state among a complete set of orthogonal ones,” *Physical Review A* **65**, 044,302 (2002). quant-ph/0105046, URL <http://dx.doi.org/10.1103/PhysRevA.65.044302>.
- [13] K. Svozil, “Quantum information in base n defined by state partitions,” *Physical Review A* **66**, 044,306 (2002). quant-ph/0205031, URL <http://dx.doi.org/10.1103/PhysRevA.66.044306>.
- [14] E. Farhi, J. Goldstone, S. Gutmann, and M. Sipser, “Limit on the Speed of Quantum Computation in Determining Parity,” *Physical Review Letters* **81**, 5442–5444 (1998). quant-ph/9802045, URL <http://dx.doi.org/10.1103/PhysRevLett.81.5442>.
- [15] X. Miao, “A polynomial-time solution to the parity problem on an NMR quantum computer,” (2001). quant-ph/0108116.
- [16] R. Orus, J. I. Latorre, and M. A. Martin-Delgado, “Systematic Analysis of Majorization in Quantum Algorithms,” *European Physical Journal D* **29**, 119–132 (2004). quant-ph/0212094, URL <http://dx.doi.org/10.1140/epjd/e2004-00009-3>.
- [17] R. Stadelhofer, D. Suterand, and W. Banzhaf, “Quantum and classical parallelism in parity algorithms

for ensemble quantum computers,” Physical Review A **71**, 032,345 (2005). quant-ph/0112105, URL <http://dx.doi.org/10.1103/PhysRevA.71.032345>.